PATENT ABSTRACTS OF JAPAN

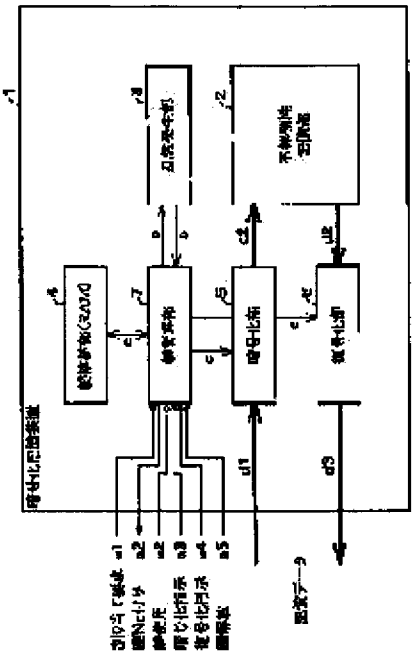
(11)Publication number : **2002-268946**
(43)Date of publication of application : **20.09.2002**

(51)Int.Cl. G06F 12/14
G11B 20/10
G11B 27/00

(21)Application number : **2001-067700**
(22)Date of filing : **09.03.2001**

(71)Applicant : **SHARP CORP**
(72)Inventor : **OBARA RYOKO**
HAMADA AKIRA

(54) DATA STORAGE DEVICE



(57)Abstract:
PROBLEM TO BE SOLVED: To provide a data storage device capable of suppressing chain discrimination of stored data of a nonvolatile storage device by persons not concerned.
SOLUTION: In an encryption storage device 1, a key managing part 7 outputs a generation request signal b to a random number generating part 3 when an allocation request signal a1 is inputted. The random number generating part 3 generates a pseudo random number at input timing of the generation request signal b, adopts it as an encryption key, the key managing part 7 stores the encryption key c into a volatile key storage part 4 and returns a corresponding key number a2 to the user side. When the user inputs an encryption instruction signal a3 and the key number a2 to the key managing part 7, the key managing part 7 reads a corresponding encryption key c, an encrypting part 5 converts data d1 to be inputted into encrypted data d2 and stores it in a nonvolatile storage part 2. When the user inputs a decryption instruction signal a4 and the key number a2 to the key managing part 7, the key managing part 7 reads the corresponding key number c and a decrypting part 6 converts the encrypted data into decrypted data d3.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－268946
（P2002－268946A）
(43)公開日　平成14年９月20日(2002.9.20)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　12/14	３２０	Ｃ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
Ｇ１１Ｂ　20/10		Ｃ１１Ｂ　20/10	Ｈ	５Ｄ０４４
27/00		27/00	Ｄ	５Ｄ１１０

審査請求　未請求　請求項の数９　ＯＬ　（全 14 頁）

(21)出願番号　特願2001－67700(P2001－67700)

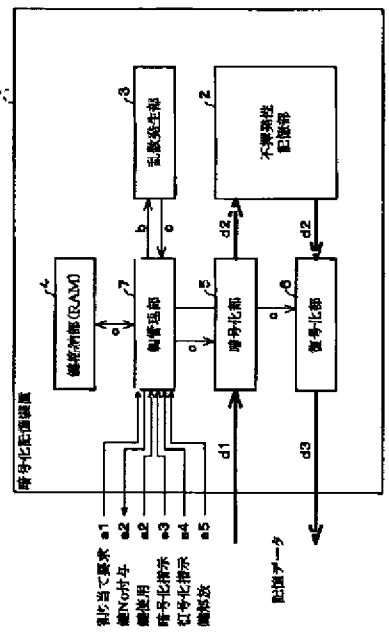
(22)出願日　平成13年３月９日(2001.3.9)

(71)出願人　000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町22番22号
(72)発明者　小原　良子
大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内
(72)発明者　濱田　明
大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内
(74)代理人　100080034
弁理士　原　謙三

最終頁に続く

(54)【発明の名称】　データ記憶装置

(57)【要約】
【課題】　非関係者に不揮発性の記憶装置の記憶データが連鎖的に判別されるのを抑制することのできるデータ記憶装置を提供する。
【解決手段】　暗号化記憶装置１において、鍵管理部７は割り当て要求信号ａ１が入力されると乱数発生部３に生成要求信号ｂを出力する。乱数発生部３は生成要求信号ｂの入力タイミングで擬似乱数を生成してこれを暗号鍵ｃとし、鍵管理部７は該暗号鍵ｃを揮発性の鍵格納部４に記憶させるとともに、対応する鍵番号ａ２を使用者側へ返す。使用者が暗号化指示信号ａ３と鍵番号ａ２とを鍵管理部７に入力すると、鍵管理部７は対応する暗号鍵ｃを読み出し、暗号化部５が入力されるデータｄ１を暗号化データｄ２に変換して不揮発性記憶部２に記憶させる。使用者が復号化指示信号ａ４と鍵番号ａ２とを鍵管理部７に入力すると、鍵管理部７は対応する暗号鍵ｃを読み出し、復号化部６が暗号化データｄ２を復号データｄ３に変換する。



【特許請求の範囲】
【請求項１】データを記憶する記憶データ不揮発性の不揮発性記憶手段を備えたデータ記憶装置において、
所定のタイミングで擬似乱数を生成し、上記タイミングごとの擬似乱数を暗号鍵とする暗号鍵発生手段と、
上記暗号鍵発生手段によって生成された上記暗号鍵を記憶する記憶データ揮発性の暗号鍵記憶手段と、
上記暗号鍵が与えられると、入力されるデータを上記暗号鍵によって暗号化して上記不揮発性記憶手段に暗号化データとして記憶させる暗号化手段と、
暗号化の際と同一の上記暗号鍵が与えられると、上記不揮発性記憶手段に記憶されている上記暗号化データを上記暗号鍵によって復号化して読み出す復号化手段と、
外部から行われる使用者への上記暗号鍵の割り当て要求に対して上記割り当て要求時に最新の上記暗号鍵に対応する暗号鍵情報を返し、入力されるデータを暗号化する指示および上記暗号鍵情報が入力されると上記暗号鍵情報に対応する上記暗号鍵を上記暗号鍵記憶手段から読み出して上記暗号化手段に与え、上記暗号化データを読み出す指示および上記暗号鍵情報が入力されると上記暗号鍵情報に対応する上記暗号鍵を上記暗号鍵記憶手段から読み出して上記復号化手段に与える暗号鍵管理手段と、
を備えていることを特徴とするデータ記憶装置。
【請求項２】上記暗号鍵発生手段は、外部からの上記暗号鍵の生成要求を受け付け、上記生成要求時を上記所定のタイミングとして上記暗号鍵を生成することを特徴とする請求項１に記載のデータ記憶装置。
【請求項３】上記暗号鍵管理手段は、上記割り当て要求時に上記暗号鍵発生手段に上記生成要求を行うことを特徴とする請求項２に記載のデータ記憶装置。
【請求項４】一定時間ごとに信号を生成するタイマーを備え、上記暗号鍵発生手段の上記所定のタイミングが上記信号の生成タイミングに連動していることを特徴とする請求項１ないし３のいずれかに記載のデータ記憶装置。
【請求項５】上記暗号鍵記憶手段に複数の上記暗号鍵が記憶されることを特徴とする請求項１ないし４のいずれかに記載のデータ記憶装置。
【請求項６】上記暗号鍵管理手段は、上記暗号鍵発生手段によって生成された最新の上記暗号鍵を上記暗号鍵記憶手段に既に記憶されている上記暗号鍵と比較して一致するものがある場合には、上記暗号鍵発生手段に最新の上記暗号鍵を一致しなくなるまで生成し直させ、一致する上記暗号鍵は使用者に割り当てないことを特徴とする請求項１ないし５のいずれかに記載のデータ記憶装置。
【請求項７】上記暗号鍵管理手段は、外部から上記暗号鍵を無効にする指示を上記暗号鍵に対応する上記暗号鍵情報との組合せで受け付けて、上記暗号鍵情報が入力されても上記暗号鍵を上記暗号化手段および上記復号化手段に与えないようにすることを特徴とする請求項１ないし６のいずれかに記載のデータ記憶装置。
【請求項８】上記暗号鍵管理手段は、上記暗号鍵の使用者への割り当てから所定時間が経過すると上記暗号鍵情報が入力されても上記暗号鍵を上記暗号化手段および上記復号化手段に与えないことを特徴とする請求項１ないし７のいずれかに記載のデータ記憶装置。
【請求項９】擬似乱数を上記暗号鍵情報として生成する暗号鍵情報発生手段を備えていることを特徴とする請求項１ないし８のいずれかに記載のデータ記憶装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、データを記憶するデータ記憶装置に関するものである。
【０００２】
【従来の技術】機密データを不揮発性の記憶媒体に記憶するデータ記憶装置は種々提案されている。
【０００３】例えば記憶されたデータの読み出しを制限するために、特開昭６２－１０７３５２号公報には、データを記憶するＲＯＭと、暗号鍵が書き込まれる揮発性メモリもしくは揮発性レジスタとを備えた暗号化ＲＯＭ装置が開示されている。この暗号化ＲＯＭ装置にデータを記憶させる場合には、揮発性メモリもしくは揮発性レジスタに暗号鍵を書き込み、該暗号鍵でデータを暗号化してＲＯＭに記憶する。また、暗号化ＲＯＭ装置からデータを読み出す場合には、揮発性メモリもしくは揮発性レジスタに暗号鍵を書き込み、該暗号鍵でＲＯＭのデータを復号化する。揮発性メモリもしくは揮発性レジスタに書き込まれた暗号鍵は、暗号化ＲＯＭ装置の電源を断にすることによって容易に消滅するので、単に電源を再投入しただけではＲＯＭのデータを読み出すことができないようになっている。
【０００４】また、既に必要がなくなった機密データについて、特開平０９－２２３０６１号公報には、機密データが格納されたハードディスクなどの情報の格納領域から、機密データの読み出し処理の終了後に、データの格納位置などを管理するＦＡＴなどのインデックスのみならず機密データをも消去して機密保持を強化しようとする情報処理装置が開示されている。
【０００５】
【発明が解決しようとする課題】しかしながら、上記特開昭６２－１０７３５２号公報の暗号化ＲＯＭ装置では、ＲＯＭに解析しやすいデータが記憶されている状態で部外者に持ち出されるなどして記憶内容が解析されると、消滅した暗号鍵が推測される虞がある。非関係者に暗号鍵が知られると、この暗号化ＲＯＭ装置に記憶されるデータが次々に復号化される危険性がある。この危険は、解析したＲＯＭに記憶されている他のデータのみならず、今後この暗号化ＲＯＭ装置に記憶されるデータにも及ぶ。
【０００６】また、特開平０９－２２３０６１号公報の

情報処理装置の場合、インデックスに加えて機密データそのものを消去するため、消去すべきデータのサイズが大きい。従って、消去に要する時間が増大することになり、情報の格納領域に対するデータ入出力の効率の低下を招く虞がある。

【０００７】本発明は、上記従来の問題点に鑑みなされたものであり、その目的は、非関係者に不揮発性の記憶媒体の記憶データが連鎖的に判別されるのを抑制することのできるデータ記憶装置を提供することにある。また、本発明の他の目的は、読み出す必要がなくなった不揮発性の記憶媒体の記憶データを、データ入出力の効率を低下させることなく非関係者に読み出し困難とすることのできるデータ記憶装置を提供することにある。

【０００８】

【課題を解決するための手段】本発明のデータ記憶装置は、上記課題を解決するために、データを記憶する記憶データ不揮発性の不揮発性記憶手段を備えたデータ記憶装置において、所定のタイミングで擬似乱数を生成し、上記タイミングごとの擬似乱数を暗号鍵とする暗号鍵発生手段と、上記暗号鍵発生手段によって生成された上記暗号鍵を記憶する記憶データ揮発性の暗号鍵記憶手段と、上記暗号鍵が与えられると、入力されるデータを上記暗号鍵によって暗号化して上記不揮発性記憶手段に暗号化データとして記憶させる暗号化手段と、暗号化の際と同一の上記暗号鍵が与えられると、上記不揮発性記憶手段に記憶されている上記暗号化データを上記暗号鍵によって復号化して読み出す復号化手段と、外部から行われる使用者への上記暗号鍵の割り当て要求に対して上記割り当て要求時に最新の上記暗号鍵に対応する暗号鍵情報を返し、入力されるデータを暗号化する指示および上記暗号鍵情報が入力されると上記暗号鍵情報に対応する上記暗号鍵を上記暗号鍵記憶手段から読み出して上記暗号化手段に与え、上記暗号化データを読み出す指示および上記暗号鍵情報が入力されると上記暗号鍵情報に対応する上記暗号鍵を上記暗号鍵記憶手段から読み出して上記復号化手段に与える暗号鍵管理手段と、を備えていることを特徴としている。

【０００９】上記の発明によれば、暗号鍵発生手段が所定のタイミングで擬似乱数を発生して各タイミングでの擬似乱数を暗号鍵とし、暗号鍵記憶手段がこの暗号鍵を記憶する。そして、暗号鍵管理手段は、外部から使用者が暗号鍵の割り当てを要求してきたときに最新の暗号鍵に対応する暗号鍵情報を使用者に返す。使用者によってデータの暗号化の指示と暗号鍵情報とが入力されると、その暗号鍵情報に対応する暗号鍵を暗号鍵記憶手段から読み出して暗号化手段に与える。暗号化手段は入力されるデータを与えられた暗号鍵によって暗号化して不揮発性記憶手段、すなわち不揮発性の記憶媒体に暗号化データとして記憶させる。

【００１０】また、暗号鍵管理手段は、使用者によって暗号化データを読み出す指示および暗号鍵情報が入力されると、その暗号鍵情報に対応する暗号鍵を暗号鍵記憶手段から読み出して復号化手段に与える。復号化手段は、暗号化の際と同一の暗号鍵が与えられると、不揮発性記憶手段に記憶されている暗号化データを暗号鍵によって復号化して読み出す。

【００１１】このように、擬似乱数を暗号鍵とするので、複数の暗号鍵を生成すると同一の暗号鍵が生じる確率は極めて小さくなる。従って、生成された最新の暗号鍵を使用者に割り当てることにより、擬似乱数の異なる生成タイミングを経て割り当てられる複数の暗号鍵を高い確率で異ならせることができる。これにより、様々な暗号鍵によるデータの暗号化および復号化を容易に行うことができるようになり、不揮発性記憶手段には暗号鍵の異なる複数の暗号化データを記憶させることができる。

【００１２】また、暗号鍵記憶手段は記憶データ揮発性であるので、持ち出されるなどしてデータが解析される場合には、通常電源が遮断されて暗号鍵記憶手段に記憶されていた暗号鍵は消滅する。この状態で不揮発性記憶手段に記憶されている暗号化データを解析された場合、解析が容易な暗号化データが偶然存在してこの暗号化データの暗号鍵が推測されたとしても、推測された暗号鍵では、その他の異なる暗号鍵で暗号化された暗号化データを復号化することはできない。また、持ち出された不揮発性記憶手段の暗号化データについての暗号鍵が推測されたとしても、今後この不揮発性記憶手段に記憶される暗号化データの暗号鍵には擬似乱数が使用されるので、推測されたものとは異なる確率が非常に高い。従って、暗号化データが使用者以外に連鎖的に判別されることはほとんどない。

【００１３】この結果、非関係者に不揮発性の記憶媒体の記憶データが連鎖的に判別されるのを抑制することのできるデータ記憶装置を提供することができる。

【００１４】また、使用者により不揮発性記憶手段に記憶されている暗号化データの復号化が行われた後など、暗号化データをこれ以上読み出す必要がなくなった場合に、上述したように非関係者による暗号鍵の推測は、解析が容易なデータでない限り困難である。従って、不揮発性記憶手段に記憶されている暗号化データを消去するといった、データ入出力の妨げとなる時間のかかる作業は不要である。この結果、読み出す必要がなくなった不揮発性の記憶媒体の記憶データを、データ入出力の効率を低下させることなく非関係者に読み出し困難とすることのできるデータ記憶装置を提供することができる。

【００１５】さらに本発明のデータ記憶装置は、上記課題を解決するために、上記暗号鍵発生手段は、外部からの上記暗号鍵の生成要求を受け付け、上記生成要求時を上記所定のタイミングとして上記暗号鍵を生成することを特徴としている。

【００１６】上記の発明によれば、暗号鍵を生成したいときに暗号鍵発生手段に暗号鍵を生成させるので、既に生成されて暗号鍵記憶手段に記憶されている暗号鍵とは異なる暗号鍵を容易に得ることができる。また、無駄な暗号鍵の生成を避けることができる。

【００１７】さらに本発明のデータ記憶装置は、上記課題を解決するために、上記暗号鍵管理手段は、上記割り当て要求時に上記暗号鍵発生手段に上記生成要求を行うことを特徴としている。

【００１８】上記の発明によれば、暗号鍵の割り当て要求時に暗号鍵発生手段に暗号鍵を生成させるので、割り当て要求ごとに異なる暗号鍵を容易に得ることができる。従って、データを他の使用者に判別されにくいものとしたり、同一使用者の読み出し対象としていないデータが読み出されてしまうことを避けたりすることができる。また、暗号鍵の生成要求を別途行わなくてもすむ。

【００１９】さらに本発明のデータ記憶装置は、上記課題を解決するために、一定時間ごとに信号を生成するタイマーを備え、上記暗号鍵発生手段の上記所定のタイミングが上記信号の生成タイミングに連動していることを特徴としている。

【００２０】上記の発明によれば、放置しておいても暗号鍵発生手段に暗号鍵を次々に生成させることができるので、暗号鍵の生成のきっかけを意図的に与える必要がない。

【００２１】さらに本発明のデータ記憶装置は、上記課題を解決するために、上記暗号鍵記憶手段に複数の上記暗号鍵が記憶されることを特徴としている。

【００２２】上記の発明によれば、暗号鍵のそれぞれを別々のデータの暗号化および復号化に用いることができるので、同じ期間に異なる使用者に異なる暗号鍵を割り当てたり、同一使用者に異なるデータの処理用に異なる暗号鍵を割り当てたりすることができる。従って、同じ期間に各データの機密保持が確保された状態での不揮発性記憶手段の使用可能回数が増加し、データの暗号化および復号化の効率を向上させることができる。

【００２３】さらに本発明のデータ記憶装置は、上記課題を解決するために、上記暗号鍵管理手段は、上記暗号鍵発生手段によって生成された最新の上記暗号鍵を上記暗号鍵記憶手段に既に記憶されている上記暗号鍵と比較して一致するものがある場合には、上記暗号鍵発生手段に最新の上記暗号鍵を一致しなくなるまで生成し直させ、一致する上記暗号鍵は使用者に割り当てないことを特徴としている。

【００２４】上記の発明によれば、暗号鍵記憶手段に既に記憶されている暗号鍵とは異なる最新の暗号鍵が使用者に割り当てられるので、擬似乱数の異なる生成タイミングを経て割り当てられる複数の暗号鍵を確実に異ならせることができる。

【００２５】さらに本発明のデータ記憶装置は、上記課題を解決するために、上記暗号鍵管理手段は、外部から上記暗号鍵を無効にする指示を上記暗号鍵に対応する上記暗号鍵情報との組合せで受け付けて、上記暗号鍵情報が入力されても上記暗号鍵を上記暗号化手段および上記復号化手段に与えないようにすることを特徴としている。

【００２６】上記の発明によれば、暗号鍵をもう使用しないときにいつでも暗号鍵をデータの暗号化や復号化に使用不可とすることができるので、データが不用意に読み出される可能性を極力小さくすることができる。

【００２７】さらに本発明のデータ記憶装置は、上記課題を解決するために、上記暗号鍵管理手段は、上記暗号鍵の使用者への割り当てから所定時間が経過すると上記暗号鍵情報が入力されても上記暗号鍵を上記暗号化手段および上記復号化手段に与えないことを特徴としている。

【００２８】上記の発明によれば、割り当てから所定時間が経過すると暗号鍵が使用不可となるので、同じ暗号鍵が使用者に長い間占有されるのを防止することができる。また、暗号鍵を使用不可とする指示を使用者から与えなくても使用不可となるので、データが不用意に読み出される可能性を自動的に極力小さくすることができる。

【００２９】さらに本発明のデータ記憶装置は、上記課題を解決するために、擬似乱数を上記暗号鍵情報として生成する暗号鍵情報発生手段を備えていることを特徴としている。

【００３０】上記の発明によれば、暗号鍵情報が擬似乱数で使用者に与えられるので、過去に与えられた暗号鍵情報を使用したデータの不正な暗号化および復号化が行われるのを防止することができる。

【００３１】

【発明の実施の形態】〔実施の形態１〕本発明のデータ記憶装置を具現する一実施の形態について、図１ないし図７を用いて説明すれば以下の通りである。

【００３２】図１に、本実施の形態に係るデータ記憶装置としての暗号化記憶装置１の構成を示す。暗号化記憶装置１は、不揮発性記憶部２、乱数発生部３、鍵格納部４、暗号化部５、復号化部６、および鍵管理部７を備えている。

【００３３】不揮発性記憶部（不揮発性記憶手段）２はハードディスクやＲＯＭなど記憶データ不揮発性の記憶媒体である。不揮発性記憶部２には暗号化されたデータである暗号化データが記憶される。乱数発生部（暗号鍵発生手段）３は所定のタイミングで擬似乱数を生成し、該タイミングごとに生成した擬似乱数を暗号鍵ｃとする。ここでは、乱数発生部３は後述する鍵管理部７からの暗号鍵ｃの生成要求を受け、該生成要求時を所定のタイミングとする。鍵格納部（暗号鍵記憶手段）４はＲＡＭなど記憶データ揮発性の記憶媒体である。鍵格納部４

は乱数発生部３で生成された暗号鍵ｃを鍵管理部７による管理で記憶する。

【００３４】暗号化部（暗号化手段）５は、鍵管理部７から暗号鍵ｃが与えられると、暗号化記憶装置１の外部から入力されるデータｄ１を、与えられた暗号鍵ｃによって暗号化して不揮発性記憶部２に暗号化データｄ２として記憶させる。復号化部（復号化手段）６は、鍵管理部７から暗号化の際と同一の暗号鍵ｃが与えられると、不揮発性記憶部２に記憶されている暗号化データｄ２を、与えられた暗号鍵ｃによって復号化して読み出し、復号データｄ３として暗号化記憶装置１の外部に出力する。

【００３５】図２（ａ）・（ｂ）に暗号化部５および復号化部６の構成例を示す。同図（ａ）は、ＥＸ－ＯＲゲート８によって暗号化記憶装置１の外部から入力されるデータｄ１と暗号鍵ｃとの排他的論理和をとることによって暗号化データｄ２を生成する暗号化部５の構成、およびＥＸ－ＯＲゲート８によって不揮発性記憶部２の暗号化データｄ２と暗号鍵ｃとの排他的論理和をとることによって復号データｄ３を生成する復号化部６の構成である。同図（ｂ）は同図（ａ）の構成に暗号鍵ｃをトリガーとして擬似乱数ｅを生成してこの擬似乱数ｅをＥＸ－ＯＲゲート８に入力する暗号鍵乱数化部９を追加したものであり、ＥＸ－ＯＲゲート８によって上記擬似乱数ｅとデータｄ１との排他的論理和をとることによって暗号化データｄ２を生成する暗号化部５の構成、およびＥＸ－ＯＲゲート８によって上記擬似乱数ｅと暗号化データｄ２との排他的論理和をとることによって復号データｄ３を生成する復号化部６の構成である。暗号鍵乱数化部９は同じ暗号鍵ｃが入力されると常に同じ擬似乱数ｅを出力する。同図（ｂ）の構成では、暗号鍵ｃが単純な数値列であってもこれを乱数化することによって複雑な数値列に置き換え、暗号化データｄ２の解析によって暗号鍵ｃが容易に推測されないようになっている。

【００３６】鍵管理部（暗号鍵管理手段）７は、暗号鍵ｃの発生や受け渡し、選択を管理している。鍵管理部７は、暗号化記憶装置１の外部から暗号化記憶装置１の使用者によりコンピュータを介して暗号鍵ｃの割り当て要求を示す割り当て要求信号ａ１が入力されるようになっており、割り当て要求信号ａ１が入力されると乱数発生部３に暗号鍵ｃの生成要求を示す生成要求信号ｂを出力する。そして乱数発生部３で生成された暗号鍵ｃを鍵格納部４に記憶させるとともに、生成したばかりの暗号鍵ｃ、すなわち最新の暗号鍵ｃに対応する鍵番号（暗号鍵情報）ａ２を使用者側（コンピュータ）へ返す。鍵格納部４には乱数発生部３により過去に生成された暗号鍵ｃがいくつか記憶されているが、鍵番号ａ２は暗号鍵ｃごとに異なっている。

【００３７】また、鍵管理部７には、暗号化の指示を示す暗号化指示信号ａ３と、復号化の指示を示す復号化指示信号ａ４とが入力されるようになっている。使用者はデータｄ１を暗号化して不揮発性記憶部２に記憶させようとするとき、暗号化指示信号ａ３と鍵番号ａ２とをコンピュータを介して鍵管理部７に入力する。鍵管理部７はこの入力に基づいて鍵番号ａ２に対応する暗号鍵ｃを鍵格納部４から読み出して暗号化部５に与える。また、使用者は不揮発性記憶部２の暗号化データｄ２を復号化して復号データｄ３を読み出そうとするとき、復号化指示信号ａ４と鍵番号ａ２とをコンピュータを介して鍵管理部７に入力する。鍵管理部７はこの入力に基づいて鍵番号ａ２に対応する暗号鍵ｃを鍵格納部４から読み出して復号化部６に与える。また、鍵管理部７には、使用者が割り当てられた暗号鍵ｃを無効にする指示を示す鍵解放信号ａ５が入力されるようになっており、鍵管理部７は、鍵解放信号ａ５に加えてその暗号鍵ｃに対応する適正な鍵番号ａ２が入力されると、以後、その鍵番号ａ２が入力されても対応する暗号鍵ｃを暗号化部５および復号化部６に与えないようになっている。

【００３８】さらに、鍵管理部７は暗号鍵ｃの使用者への割り当て内容を表す割り当て枠を認識して、鍵格納部４に記憶させている。図３に割り当て枠の構造の一例を示す。割り当て枠は０からＮのＮ＋１個の複数の鍵番号ａ２のそれぞれに対応して設けられており、割り当て枠ごとに１つの暗号鍵ｃが対応している。なお、割り当て枠を１つとすることも可能である。そして、暗号鍵ｃ…が割り当て枠の総数であるＮ＋１個を上限として鍵格納部４に格納されるようになっている。鍵管理部７は、既に使用者に割り当て、現在有効である暗号鍵ｃの割り当て枠に使用中フラグ“１”を立てる。また、鍵管理部７は、既に使用者に割り当てたが現在無効としている暗号鍵ｃの割り当て枠、およびまだ使用者に暗号鍵ｃを割り当てていない割り当て枠に、未使用の割り当て枠であることを示すフラグ“０”を立てる。さらに、鍵管理部７は、使用中フラグ“１”を立てた割り当て枠に対して前述の鍵解放信号ａ５に基づいた暗号鍵ｃの無効化を行うと、その割り当て枠のフラグを“０”に変更する。

【００３９】上記図３の割り当て枠が設けられている状態での暗号鍵ｃの割り当て（「鍵付与」と称する）の手順を図４のフローチャートを用いて説明する。まず、割り当て要求信号ａ１が鍵管理部７に入力されると、Ｓ１で鍵管理部７は未使用の割り当て枠を検索する。Ｓ２で未使用の割り当て枠が存在する場合にはＳ３へ進み、存在しない場合にはＳ８へ進んでエラー通知を使用者側（コンピュータ）へ返して処理を終了する。Ｓ３では鍵管理部７が乱数発生部３に生成要求信号ｂを出力して乱数発生部３に暗号鍵ｃを生成させる。

【００４０】次いでＳ４で鍵管理部７は、乱数発生部３によって生成された最新の暗号鍵ｃとしての擬似乱数の値を、鍵格納部４に既に記憶されている暗号鍵ｃとしての擬似乱数の値と比較する。このとき無効とされている

暗号鍵ｃも比較対象とする。そして、鍵格納部４に既に記憶されている暗号鍵ｃの中に最新の暗号鍵ｃと一致するものがなければＳ５へ進み、一致するものがあればＳ３に戻って乱数発生部３に暗号鍵ｃを生成し直させる。従って、鍵管理部７は鍵格納部４に既に記憶されている暗号鍵ｃの中に最新の暗号鍵ｃと一致するものがなくなるまで乱数発生部３に最新の暗号鍵ｃを生成し直させる。一致した最新の暗号鍵ｃは鍵格納部４には記憶せず、自動的に使用者への割り当て対象外とする。

【００４１】Ｓ５では鍵管理部７が最新の暗号鍵ｃを設定し、鍵格納部４に記憶させる。そして、Ｓ６で最新の暗号鍵ｃを未使用の割り当て枠のいずれかの暗号鍵ｃとし、その割り当て枠のフラグを“０”から“１”に変更する。Ｓ７でその暗号鍵ｃに対応する鍵番号ａ２を使用者に返して処理が終了する。以上が鍵付与の手順である。

【００４２】次に、前記図３の割り当て枠が設けられている状態での暗号鍵ｃの無効化（「鍵解放」と称する）の手順を図５のフローチャートを用いて説明する。まず、鍵解放信号ａ５と解放しようとする暗号鍵ｃに対応する適正な鍵番号ａ２とが鍵管理部７に入力されると、Ｓ１１で鍵管理部７は上記鍵番号ａ２の割り当て枠を検索する。そしてＳ１２で鍵管理部７は検索した割り当て枠のフラグを“１”から“０”に変更（リセット）する。以上が鍵解放の手順である。

【００４３】このように、本実施の形態の暗号化記憶装置１によれば、擬似乱数を暗号鍵ｃとするので、複数の暗号鍵ｃ…を生成すると同一の暗号鍵ｃが生じる確率は極めて小さくなる。従って、生成された最新の暗号鍵ｃを使用者に割り当てることにより、擬似乱数の異なる生成タイミングを経て割り当てられる複数の暗号鍵ｃ…を高い確率で異ならせることができる。これにより、様々な暗号鍵ｃ…によるデータの暗号化および復号化を容易に行うことができるようになり、不揮発性記憶部２には暗号鍵ｃの異なる複数の暗号化データｄ２を記憶させることができる。

【００４４】特に暗号化記憶装置１では、鍵管理部７が、乱数発生部３によって生成された最新の暗号鍵ｃを鍵格納部４に既に記憶されている暗号鍵ｃ（あるいはｃ…）と比較して一致するものがある場合には、乱数発生部３に最新の暗号鍵ｃを一致しなくなるまで生成し直させ、一致する暗号鍵ｃは使用者に割り当てないようになっている。従って、鍵格納部４に既に記憶されている暗号鍵ｃ（あるいはｃ…）とは異なる最新の暗号鍵ｃが使用者に割り当てられるので、鍵管理部７が割り当て要求信号ａ１が入力されたときに生成要求信号ｂを出力して乱数発生部３に新たな暗号鍵ｃを生成させる場合のように、擬似乱数の異なる生成タイミングを経て生成された複数の暗号鍵ｃ…を使用者に割り当てることにより、暗号鍵ｃ…のそれぞれを互いに確実に異ならせることができる。

【００４５】また、鍵格納部４は記憶データ揮発性であるので、暗号化記憶装置１が持ち出されるなどしてデータが解析される場合には、通常電源が遮断されて鍵格納部４に記憶されていた暗号鍵ｃ（あるいはｃ…）は消滅する。この状態で不揮発性記憶部２に記憶されている暗号化データｄ２を解析された場合、解析が容易な暗号化データｄ２が偶然存在してこの暗号化データｄ２の暗号鍵ｃが推測されたとしても、推測された暗号鍵ｃでは、その他の異なる暗号鍵ｃで暗号化された暗号化データｄ２を復号化することはできない。また、持ち出された不揮発性記憶部２の暗号化データｄ２についての暗号鍵ｃが推測されたとしても、今後この不揮発性記憶部２に記憶される暗号化データｄ２の暗号鍵ｃには擬似乱数が使用されるので、推測されたものとは異なる確率が非常に高い。従って、暗号化データｄ２が使用者以外に連鎖的に判別されることはほとんどない。

【００４６】この結果、暗号化記憶装置１は、非関係者に不揮発性の記憶媒体の記憶データが連鎖的に判別されるのを抑制することのできるデータ記憶装置となる。

【００４７】また、使用者により不揮発性記憶部２に記憶されている暗号化データｄ２の復号化が行われた後など、暗号化データｄ２をこれ以上読み出す必要がなくなった場合に、上述したように非関係者による暗号鍵ｃの推測は、解析が容易なデータでない限り困難である。従って、不揮発性記憶部２に記憶されている暗号化データｄ２を消去するといった、データ入出力の妨げとなる時間のかかる作業は不要である。この結果、暗号化記憶装置１は、読み出す必要がなくなった不揮発性の記憶媒体の記憶データを、データ入出力の効率を低下させることなく非関係者に読み出し困難とすることのできるデータ記憶装置となる。

【００４８】また、暗号化記憶装置１によれば、乱数発生部３は、外部からの暗号鍵ｃの生成要求がそのまま反映される生成要求信号ｂを鍵管理部７から受け付け、生成要求時を所定のタイミングとして暗号鍵ｃを生成する。このように、暗号鍵ｃを生成したいときに乱数発生部３に暗号鍵ｃを生成させるので、既に生成されて鍵格納部４に記憶されている暗号鍵ｃ（あるいはｃ…）とは異なる暗号鍵ｃを容易に得ることができる。また、使用されないような無駄な暗号鍵ｃの生成を避けることができる。

【００４９】また、暗号化記憶装置１によれば、鍵管理部７が、割り当て要求信号ａ１が入力されたときに乱数発生部３に生成要求信号ｂを出力して上記の生成要求を行っている。このように、暗号鍵ｃの割り当て要求時に乱数発生部３に暗号鍵ｃを生成させるので、割り当て要求ごとに異なる暗号鍵ｃを容易に得ることができる。従って、データを他の使用者に判別されにくいものとしたり、同一使用者の読み出し対象としていないデータが読

み出されてしまうことを避けたりすることができる。また、暗号鍵ｃの生成要求を別途行わなくてもすむ。

【００５０】また、暗号化記憶装置１によれば、鍵格納部４に複数の暗号鍵ｃ…が記憶される。従って、暗号鍵ｃ…のそれぞれを別々のデータの暗号化および復号化に用いることができるので、同じ期間に異なる使用者に異なる暗号鍵ｃを割り当てたり、同一使用者に異なるデータの処理用に互いに異なる暗号鍵ｃを割り当てたりすることができる。従って、同じ期間に各データの機密保持が確保された状態での不揮発性記憶部２の使用可能回数が増加し、データの暗号化および復号化の効率を向上させることができる。

【００５１】また、暗号化記憶装置１では、鍵管理部７が、鍵解放信号ａ５のように外部から暗号鍵ｃを無効にする指示を該暗号鍵ｃに対応する鍵番号ａ２との組合せで受け付けて、鍵番号ａ２が入力されても上記暗号鍵ｃを暗号化部５および復号化部６に与えないようになっている。従って、暗号鍵ｃをもう使用しないときにいつでも暗号鍵ｃをデータの暗号化や復号化に使用不可とすることができるので、データが不用意に読み出される可能性を極力小さくすることができる。

【００５２】また、暗号化記憶装置１では、使用者に割り当てる鍵番号ａ２を擬似乱数としてもよい。例えば、暗号化記憶装置１で乱数発生部３を、擬似乱数を鍵番号ａ２として生成する暗号鍵情報発生手段としても機能させることができる。鍵番号ａ２を擬似乱数とした場合の割り当て枠の構造の一例を図６に示す。鍵番号ａ２が擬似乱数であるので、割り当て枠そのものに０からＮまでの番号が付与されている。このようにすれば、鍵番号ａ２が擬似乱数で使用者に与えられるので、過去に与えられた鍵番号ａ２が現在も使用されているのではないかと推測されて過去の鍵番号ａ２を使用したデータの不正な暗号化および復号化が行われるのを、防止することができる。

【００５３】鍵番号ａ２を擬似乱数とする場合の暗号鍵ｃの割り当て（「鍵付与」と称する）の手順を図７のフローチャートを用いて説明する。まず、割り当て要求信号ａ１が鍵管理部７に入力されると、Ｓ２１で鍵管理部７は未使用の割り当て枠を検索する。Ｓ２２で未使用の割り当て枠が存在する場合にはＳ２３へ進み、存在しない場合にはＳ３０へ進んでエラー通知を使用者側（コンピュータ）へ返して処理を終了する。Ｓ２３では鍵管理部７が乱数発生部３に生成要求信号ｂを出力して乱数発生部３に鍵番号ａ２用の擬似乱数と暗号鍵ｃ用の擬似乱数とを生成させる。

【００５４】次いで「暗号鍵枠のループ」に入り、Ｓ２４で鍵管理部７は、乱数発生部３によって生成された鍵番号ａ２としての擬似乱数の値を、鍵格納部４や図示しない鍵番号ａ２用の記憶手段に既に格納されている鍵番号ａ２（あるいはａ２…）としての擬似乱数の値と比較する。比較対象を暗号化記憶装置１の電源の遮断で消滅させたくない場合は、鍵番号ａ２用の記憶手段として不揮発性の記憶媒体をどこかに設ければよい。そして、既に記憶されている鍵番号ａ２（あるいはａ２…）の中に生成されたばかりの鍵番号ａ２と一致するものがなければＳ２５へ進み、一致するものがあればＳ２３に戻って乱数発生部３に鍵番号ａ２を生成し直させる。Ｓ２５では鍵管理部７は、乱数発生部３によって生成された最新の暗号鍵ｃを、鍵格納部４に既に記憶されている暗号鍵ｃ（あるいはｃ…）と比較する。そして、鍵格納部４に既に記憶されている暗号鍵ｃ（あるいはｃ…）の中に生成された最新の暗号鍵ｃと一致するものがなければ「暗号鍵枠のループ」を抜けてＳ２６へ進み、一致するものがあればＳ２３に戻って乱数発生部３に暗号鍵ｃを生成し直させる。このとき無効とされている暗号鍵ｃも比較対象とする。鍵管理部７は、一致した最新の暗号鍵ｃを鍵格納部４には記憶させず、自動的に使用者への割り当て対象外とする。

【００５５】Ｓ２６では鍵管理部７が鍵番号ａ２を設定して記憶させ、Ｓ２７では鍵管理部７が最新の暗号鍵ｃを設定して鍵格納部４に記憶させる。そして、Ｓ２８で鍵管理部７が鍵番号ａ２および最新の暗号鍵ｃを未使用の割り当て枠のいずれかの鍵番号ａ２および暗号鍵ｃとし、その割り当て枠のフラグを“０”から“１”に変更する。Ｓ２９で鍵管理部７が、設定した鍵番号ａ２を使用者に返すと処理が終了する。以上が鍵付与の手順である。

【００５６】〔実施の形態２〕本発明のデータ記憶装置を具現する他の実施の形態について図８ないし図１５を用いて説明すれば以下の通りである。なお、前記実施の形態１で述べた構成要素と同一の機能を有する構成要素については同一の符号を付し、その説明を省略する。

【００５７】図８に、本実施の形態に係るデータ記憶装置としての暗号化記憶装置１１の構成を示す。暗号化記憶装置１１は、実施の形態１で述べた暗号化記憶装置１にタイマー１２を追加した構成である。タイマー１２は、一定時間ごとに信号ｆを生成して鍵管理部７に入力する。鍵管理部７は信号ｆが入力されると生成要求信号ｂを乱数発生部３に入力し、乱数発生部３は生成要求信号ｂの入力タイミングを前記所定のタイミングとして暗号鍵ｃを生成する。すなわち、乱数発生部３の前記所定のタイミングはタイマー１２の信号ｆの生成タイミングに連動している。

【００５８】このようなタイマー１２を備える構成における割り当て枠の構造の一例を図９に示す。鍵番号ａ２は０からＮまであり、従って割り当て枠も同数存在し、それぞれに１つの暗号鍵ｃが対応する。鍵管理部７は、タイマー１２が信号ｆを生成するごとに異なる割り当て枠に順に暗号鍵ｃを当てはめていく。タイマー１２によって信号ｆが生成されると、次の信号ｆが生成されるま

では同じ暗号鍵ｃが最新の暗号鍵ｃとなり、鍵管理部７は、最新の暗号鍵ｃに対応する鍵番号ａ２を現在の鍵番号ａ２として認識する。そして、暗号鍵ｃの割り当て（「鍵付与」と称する）を図１０のフローチャートを用いて説明すると、使用者側（コンピュータ）から鍵管理部７へ割り当て要求信号ａ１が入力されると、Ｓ４１で鍵管理部７が使用者側（コンピュータ）へ現在の鍵番号ａ２を返す（通知する）という手順になる。鍵管理部７は、現在の鍵番号ａ２を順に更新して割り当て枠が一巡すると、次の更新時には初めの割り当て枠の暗号鍵ｃを最新の暗号鍵ｃに書き替えるといったように、一定時間ごとに現在の鍵番号ａ２の割り当て枠を継続して変更する。

【００５９】図９の割り当て枠を用いる場合の、現在の鍵番号ａ２の設定（「鍵更新」と称する）の手順を図１１のフローチャートを用いて説明する。まず、タイマー１２から鍵管理部７に信号ｆが入力されると、Ｓ５１で鍵管理部７は次の現在の鍵番号ａ２を計算する。Ｓ５２で、鍵管理部７は計算した鍵番号ａ２がその時点で暗号化あるいは復号化に使用されているか否かを判定し、暗号化あるいは復号化に使用されていない場合にはＳ５５へ進み、暗号化あるいは復号化に使用されている場合にはＳ５３へ進んでエラー通知を使用者側（コンピュータ）へ行い、Ｓ５４で使用中の鍵番号ａ２の使用が完了するまで待ってＳ５５へ進む。Ｓ５５では鍵管理部７が乱数発生部３に生成要求信号ｂを入力して暗号鍵ｃを生成させる。

【００６０】Ｓ５６では鍵管理部７が、乱数発生部３によって生成された最新の暗号鍵ｃとしての擬似乱数の値を、鍵格納部４に既に記憶されている暗号鍵ｃ（あるいはｃ…）としての擬似乱数の値と比較する。そして、鍵格納部４に既に記憶されている暗号鍵ｃ（あるいはｃ…）の中に生成された最新の暗号鍵ｃと一致するものがなければＳ５７へ進み、一致するものがあればＳ５５に戻って乱数発生部３に暗号鍵ｃを生成し直させる。そして鍵管理部７は、Ｓ５７で最新の暗号鍵ｃを設定して鍵格納部４に記憶させ、Ｓ５８で現在の鍵番号ａ２を更新し、Ｓ５９で一定時間、すなわちタイマー１２から次の信号ｆが入力されるまで待つ。次の信号ｆが入力されるとＳ５１へ戻る。以上が鍵更新の手順である。

【００６１】以上に述べた暗号化記憶装置１１によれば、放置しておいても乱数発生部３に暗号鍵ｃを次々に生成させることができるので、暗号鍵ｃの生成のきっかけを使用者側が意図的に与える必要がない。

【００６２】なお、暗号化記憶装置１１において、鍵管理部７が、暗号鍵ｃを使用者へ割り当ててから所定時間が経過すると、鍵番号ａ２が入力されてもその鍵番号ａ２に対応する暗号鍵ｃを暗号化部５および復号化部６に与えないようにすることもできる。このようにすれば、割り当てから所定時間が経過すると暗号鍵ｃが使用不可となるので、同じ暗号鍵ｃが使用者に長い間占有されるのを防止することができる。また、暗号鍵ｃを使用不可とする指示を使用者から与えなくても使用不可となるので、不揮発性記憶部２から暗号化データｄ２が不用意に読み出される可能性を自動的に極力小さくすることができる。

【００６３】このように暗号鍵ｃを使用不可とするには、例えば暗号化記憶装置１１に時計を備え、鍵番号ａ２の付与（暗号鍵ｃの割り当て）の日時を記憶しておき、記憶した日時から所定時間が経過したときに鍵管理部７が割り当て枠の該当する暗号鍵ｃを無効にすることで実現することができる。なお、このような構成は実施の形態１で述べた暗号化記憶装置１や、後述する暗号化記憶装置２１にも適用することができる。

【００６４】上記時計を備えた構成の場合の、割り当て枠の構造の一例を図１２に示す。０からＮまでの鍵番号ａ２の各割り当て枠に、暗号鍵ｃと対で、暗号鍵ｃの割り当て日時（必要に応じて年月）が鍵番号ａ２の使用開始日時を示す情報として記憶される。使用開始日時から所定時間が経過した鍵番号ａ２の割り当て枠には、鍵管理部７によって使用開始日時の情報が消去されてフラグ“０”に変更（リセット）される。

【００６５】図１２の割り当て枠を用いる場合の、暗号鍵ｃの無効化（「鍵強制解放」と称する）の手順を図１３のフローチャートに示す。まず「暗号鍵枠のループ」に入り、Ｓ６１で鍵管理部７が鍵番号ａ２の付与（暗号鍵ｃの割り当て）から所定時間が経過したか否かを判定し、経過していればＳ６２へ進み、経過していなければ「暗号鍵枠のループ」を抜けてＳ６６へ進む。Ｓ６２では鍵管理部７が、所定時間が経過した鍵番号ａ２（暗号鍵ｃ）がその時点で暗号化あるいは復号化に使用されているか否かを判定し、暗号化あるいは復号化に使用されていなければＳ６５へ進む。一方、暗号化あるいは復号化に使用されていればＳ６３で使用者側（コンピュータ）にエラー通知を行い、Ｓ６４で使用中の鍵番号ａ２（暗号鍵ｃ）の使用が完了するまで待ってＳ６５へ進む。Ｓ６５では鍵管理部７が該当する鍵番号ａ２の割り当て枠の使用開始日時の情報をフラグ“０”に変更（リセット）する。これで「暗号鍵枠のループ」を抜け、Ｓ６６で前記所定時間が経過するまで待ってＳ６１に戻る。以上が鍵強制解放のので順である。

【００６６】次に、図１４に、前記暗号化記憶装置１１の変形例である暗号化記憶装置（データ記憶装置）２１の構成を示す。暗号化記憶装置２１は、暗号化記憶装置１１にセレクタ２２・２３を追加した構成である。セレクタ２２は暗号化記憶装置２１のデータｄ１の入力側と暗号化部５および復号化部６との間に設けられる。セレクタ２３は暗号化部５および復号化部６と不揮発性記憶部２との間に設けられる。セレクタ２２・２３には、暗号化の要否を示す暗号化要否信号ｇと、復号化の要否を示

す復号化要否信号ｈとが使用者側（コンピュータ）から入力されるようになっている。

【００６７】データｄ１の暗号化を行う際には、セレクタ２２・２３に暗号化を要求することを示す暗号化要否信号ｇが入力され、セレクタ２２は暗号化記憶装置２１に入力されるデータｄ１が暗号化部５に入力されるように経路を切り替え、セレクタ２３は暗号化部５から出力される暗号化データｄ２が不揮発性記憶部２に入力されるように経路を切り替える。データｄ２の復号化を行う際には、セレクタ２２・２３に復号化を要求することを示す復号化要否信号ｈが入力され、セレクタ２３は不揮発性記憶部２から出力される暗号化データｄ２が復号化部６に入力されるように経路を切り替え、セレクタ２２は復号化部６から出力される復号データｄ３が暗号化記憶装置２１から使用者側（コンピュータ）に出力されるように経路を切り替える。

【００６８】また、暗号化を行わないデータｄ１については、不揮発性記憶部２への記憶の際に、セレクタ２２・２３に暗号化を要求しないことを示す暗号化要否信号ｇが入力され、セレクタ２２・２３は、データｄ１がセレクタ２２から直接セレクタ２３に渡されて不揮発性記憶部２へ入力されるように経路を切り替える。また、この暗号化しなかったデータｄ１を不揮発性記憶部２から読み出す際には、セレクタ２２・２３に復号化を要求しないことを示す復号化要否信号ｈが入力され、セレクタ２２・２３は、データｄ１がセレクタ２３から直接セレクタ２２に渡されて暗号化記憶装置２１から使用者側（コンピュータ）に出力されるように経路を切り替える。

【００６９】上記暗号化記憶装置２１を用いたデータの読み書きの手順を、図１５のフローチャートを用いて説明する。まずＳ７１で鍵管理部７はデータ読み書きの処理中であるか否かを判定し、データ読み書きの処理中でなければＳ７２に進む。一方、データ読み書きの処理中であればＳ７９へ進んで使用者にビジー通知を行って処理を終了する。Ｓ７２で鍵管理部７はデータの暗号化あるいは復号化を行うか否かを判定し、データの暗号化あるいは復号化を行う場合にはＳ７３へ進む。一方、データの暗号化あるいは復号化を行わない場合にはＳ７７へ進んで暗号化を要求しないことを示す暗号化要否信号ｇ、あるいは復号化を要求しないことを示す復号化要否信号ｈをセレクタ２２・２３に入力してセレクタ２２とセレクタ２３とが直接つながるように経路を切り替え、Ｓ７８へ進む。

【００７０】Ｓ７３では鍵管理部７が使用者側（コンピュータ）から鍵番号ａ２を受け取り、Ｓ７４で鍵管理部７が対応する暗号鍵ｃを鍵格納部４から検索して読み出す。Ｓ７５では鍵管理部７が暗号化部５あるいは復号化部６に暗号鍵ｃを与える（セットする）。Ｓ７６では暗号化を要求することを示す暗号化要否信号ｇ、あるいは復号化を要求することを示す復号化要否信号ｈをセレクタ２２・２３に入力して、セレクタ２２・２３に暗号化用あるいは復号化用の経路に切り替えさせる。そして、Ｓ７８でデータの読み書きを行って処理を終了する。

【００７１】このように、暗号化記憶装置２１によれば、セレクタ２２・２３が設けられているので、暗号化および復号化しないデータをも不揮発性記憶部２に記憶させることができる。

【００７２】

【発明の効果】本発明のデータ記憶装置は、以上のように、所定のタイミングで擬似乱数を生成し、上記タイミングごとの擬似乱数を暗号鍵とする暗号鍵発生手段と、上記暗号鍵発生手段によって生成された上記暗号鍵を記憶する記憶データ揮発性の暗号鍵記憶手段と、上記暗号鍵が与えられると、入力されるデータを上記暗号鍵によって暗号化して上記不揮発性記憶手段に暗号化データとして記憶させる暗号化手段と、暗号化の際と同一の上記暗号鍵が与えられると、上記不揮発性記憶手段に記憶されている上記暗号化データを上記暗号鍵によって復号化して読み出す復号化手段と、外部から行われる使用者への上記暗号鍵の割り当て要求に対して上記割り当て要求時に最新の上記暗号鍵に対応する暗号鍵情報を返し、入力されるデータを暗号化する指示および上記暗号鍵情報が入力されると上記暗号鍵情報に対応する上記暗号鍵を上記暗号鍵記憶手段から読み出して上記暗号化手段に与え、上記暗号化データを読み出す指示および上記暗号鍵情報が入力されると上記暗号鍵情報に対応する上記暗号鍵を上記暗号鍵記憶手段から読み出して上記復号化手段に与える暗号鍵管理手段と、を備えている構成である。

【００７３】それゆえ、生成された最新の暗号鍵を使用者に割り当てることにより、擬似乱数の異なる生成タイミングを経て割り当てられる複数の暗号鍵を高い確率で異ならせることができる。これにより、様々な暗号鍵によるデータの暗号化および復号化を容易に行うことができるようになり、不揮発性記憶手段には暗号鍵の異なる複数の暗号化データを記憶させることができる。

【００７４】また、暗号鍵記憶手段は記憶データ揮発性であるので、持ち出されるなどしてデータが解析される場合には、通常電源が遮断されて暗号鍵記憶手段に記憶されていた暗号鍵は消滅する。この状態で不揮発性記憶手段に記憶されている暗号化データを解析された場合、解析が容易な暗号化データが偶然存在してこの暗号化データの暗号鍵が推測されたとしても、推測された暗号鍵では、その他の異なる暗号鍵で暗号化された暗号化データを復号化することはできない。また、持ち出された不揮発性記憶手段の暗号化データについての暗号鍵が推測されたとしても、今後この不揮発性記憶手段に記憶される暗号化データの暗号鍵には擬似乱数が使用されるので、推測されたものとは異なる確率が非常に高い。従って、暗号化データが使用者以外に連鎖的に判別されるこ

とはほとんどない。

【0075】この結果、非関係者に不揮発性の記憶媒体の記憶データが連鎖的に判別されるのを抑制することのできるデータ記憶装置を提供することができるという効果を奏する。

【0076】また、使用者が暗号化データをこれ以上読み出す必要がなくなった場合に、上述したように非関係者による暗号鍵の推測は、解析が容易なデータでない限り困難である。従って、不揮発性記憶手段に記憶されている暗号化データを消去するといった、データ入出力の妨げとなる時間のかかる作業は不要である。この結果、読み出す必要がなくなった不揮発性の記憶媒体の記憶データを、データ入出力の効率を低下させることなく非関係者に読み出し困難とすることのできるデータ記憶装置を提供することができるという効果を奏する。

【0077】さらに本発明のデータ記憶装置は、以上のように、上記暗号鍵発生手段は、外部からの上記暗号鍵の生成要求を受け付け、上記生成要求時を上記所定のタイミングとして上記暗号鍵を生成する構成である。

【0078】それゆえ、暗号鍵を生成したいときに暗号鍵発生手段に暗号鍵を生成させるので、既に生成されて暗号鍵記憶手段に記憶されている暗号鍵とは異なる暗号鍵を容易に得ることができるという効果を奏する。また、無駄な暗号鍵の生成を避けることができるという効果を奏する。

【0079】さらに本発明のデータ記憶装置は、以上のように、上記暗号鍵管理手段は、上記割り当て要求時に上記暗号鍵発生手段に上記生成要求を行う構成である。

【0080】それゆえ、割り当て要求ごとに異なる暗号鍵を容易に得ることができる。従って、データを他の使用者に判別されにくいものとしたり、同一使用者の読み出し対象としていないデータが読み出されてしまうことを避けたりすることができるという効果を奏する。また、暗号鍵の生成要求を別途行わなくてもすむという効果を奏する。

【0081】さらに本発明のデータ記憶装置は、以上のように、一定時間ごとに信号を生成するタイマーを備え、上記暗号鍵発生手段の上記所定のタイミングが上記信号の生成タイミングに連動している構成である。

【0082】それゆえ、放置しておいても暗号鍵発生手段に暗号鍵を次々に生成させることができるので、暗号鍵の生成のきっかけを意図的に与える必要がないという効果を奏する。

【0083】さらに本発明のデータ記憶装置は、以上のように、上記暗号鍵記憶手段に複数の上記暗号鍵が記憶される構成である。

【0084】それゆえ、暗号鍵のそれぞれを別々のデータの暗号化および復号化に用いることができるので、同じ期間に異なる使用者に異なる暗号鍵を割り当てたり、同一使用者に異なるデータの処理用に異なる暗号鍵を割り当てたりすることができる。従って、同じ期間に各データの機密保持が確保された状態での不揮発性記憶手段の使用可能回数が増加し、データの暗号化および復号化の効率を向上させることができるという効果を奏する。

【0085】さらに本発明のデータ記憶装置は、以上のように、上記暗号鍵管理手段は、上記暗号鍵発生手段によって生成された最新の上記暗号鍵を上記暗号鍵記憶手段に既に記憶されている上記暗号鍵と比較して一致するものがある場合には、上記暗号鍵発生手段に最新の上記暗号鍵を一致しなくなるまで生成し直させ、一致する上記暗号鍵は使用者に割り当てない構成である。

【0086】それゆえ、暗号鍵記憶手段に既に記憶されている暗号鍵とは異なる最新の暗号鍵が使用者に割り当てられるので、擬似乱数の異なる生成タイミングを経て割り当てられる複数の暗号鍵を確実に異ならせることができるという効果を奏する。

【0087】さらに本発明のデータ記憶装置は、以上のように、上記暗号鍵管理手段は、外部から上記暗号鍵を無効にする指示を上記暗号鍵に対応する上記暗号鍵情報との組合せで受け付けて、上記暗号鍵情報が入力されても上記暗号鍵を上記暗号化手段および上記復号化手段に与えないようにする構成である。

【0088】それゆえ、暗号鍵をもう使用しないときにいつでも暗号鍵をデータの暗号化や復号化に使用不可とすることができるので、データが不用意に読み出される可能性を極力小さくすることができるという効果を奏する。

【0089】さらに本発明のデータ記憶装置は、以上のように、上記暗号鍵管理手段は、上記暗号鍵の使用者への割り当てから所定時間が経過すると上記暗号鍵情報が入力されても上記暗号鍵を上記暗号化手段および上記復号化手段に与えない構成である。

【0090】それゆえ、割り当てから所定時間が経過すると暗号鍵が使用不可となるので、同じ暗号鍵が使用者に長い間占有されるのを防止することができるという効果を奏する。また、暗号鍵を使用不可とする指示を使用者から与えなくても使用不可となるので、データが不用意に読み出される可能性を自動的に極力小さくすることができるという効果を奏する。

【0091】さらに本発明のデータ記憶装置は、以上のように、擬似乱数を上記暗号鍵情報として生成する暗号鍵情報発生手段を備えている構成である。

【0092】それゆえ、暗号鍵情報が擬似乱数で使用者に与えられるので、過去に与えられた暗号鍵情報を使用したデータの不正な暗号化および復号化が行われるのを防止することができるという効果を奏する。

【図面の簡単な説明】

【図1】本発明の一実施の形態に係るデータ記憶装置の構成を示すブロック図である。

【図2】（a）および（b）は、図1のデータ記憶装置

の暗号化部および復号化部の構成を示す回路ブロック図である。

【図３】図１のデータ記憶装置に用いられる割り当て枠の構造例を説明する説明図である。

【図４】図３の割り当て枠を用いた場合の鍵付与の手順を示すフローチャートである。

【図５】図３の割り当て枠を用いた場合の鍵解放の手順を示すフローチャートである。

【図６】図１のデータ記憶装置に用いられる割り当て枠の他の構造例を説明する説明図である。

【図７】図６の割り当て枠を用いた場合の鍵付与の手順を示すフローチャートである。

【図８】本発明の他の実施の形態に係るデータ記憶装置の構成を示すブロック図である。

【図９】図８のデータ記憶装置に用いられる割り当て枠の構造例を説明する説明図である。

【図１０】図９の割り当て枠を用いた場合の鍵付与の手順を示すフローチャートである。

【図１１】図９の割り当て枠を用いた場合の鍵更新の手順を示すフローチャートである。

【図１２】図８のデータ記憶装置に用いられる割り当て枠の他の構造例を説明する説明図である。

【図１３】図１２の割り当て枠を用いた場合の鍵強制解放の手順を示すフローチャートである。

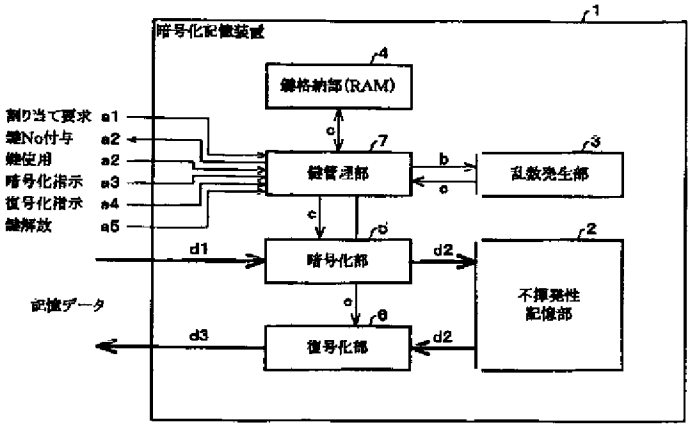
【図１４】本発明の他の実施の形態に係るデータ記憶装置の変形例の構成を示すブロック図である。

【図１５】図１４のデータ記憶装置を用いた場合のデータの読み書きの手順を示すフローーチャートである。

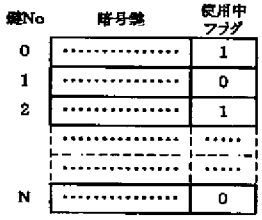
【符号の説明】

１	暗号化記憶装置（データ記憶装置）
２	不揮発性記憶部（不揮発性記憶手段）
３	乱数発生部（暗号鍵発生手段、暗号鍵情報発生手段）
４	鍵格納部（暗号鍵記憶手段）
５	暗号化部（暗号化手段）
６	復号化部（復号化手段）
７	鍵管理部（暗号鍵管理手段）
１１	暗号化記憶装置（データ記憶装置）
１２	タイマー
２１	暗号化記憶装置（データ記憶装置）
ａ２	鍵番号（暗号鍵情報）
ｃ	暗号鍵
ｄ１	データ
ｄ２	暗号化データ
ｆ	信号

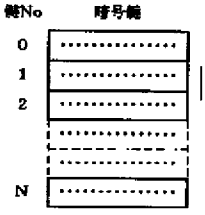
【図１】



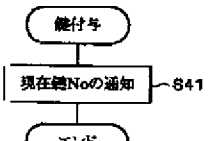
【図３】



【図９】

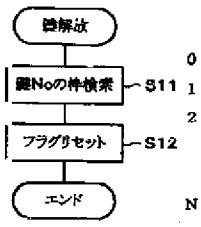


【図１０】



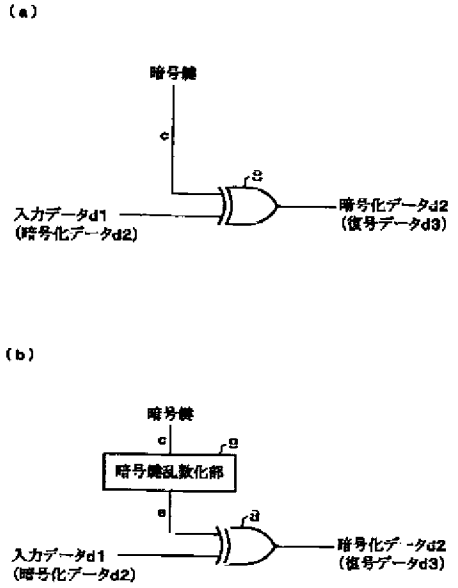
現在鍵No 2

【図５】

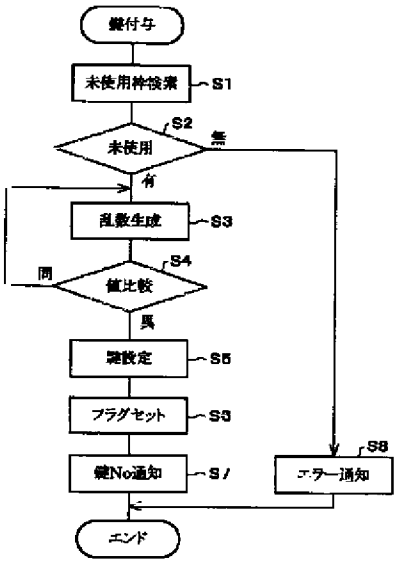


【図６】

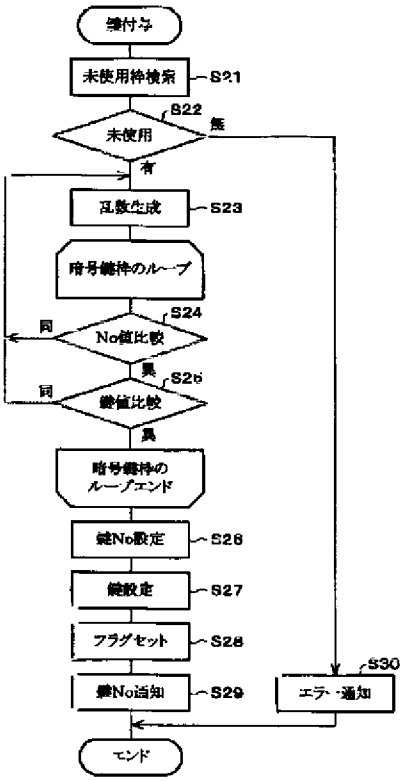
【図２】



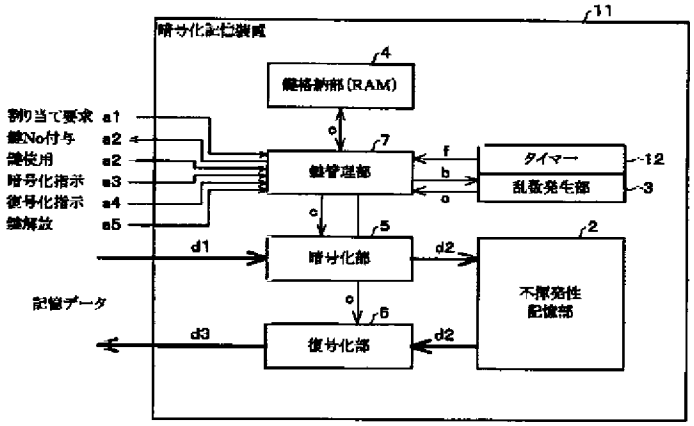
【図４】



【図７】



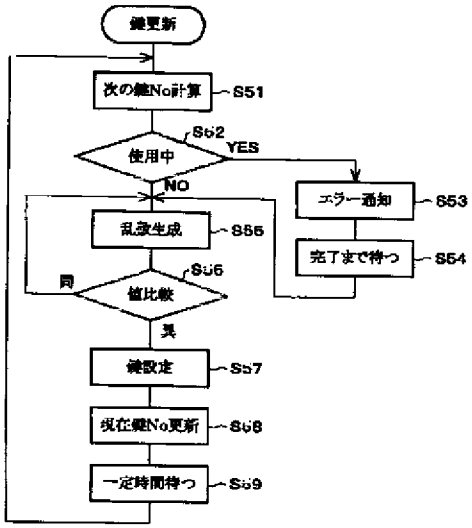
【図８】



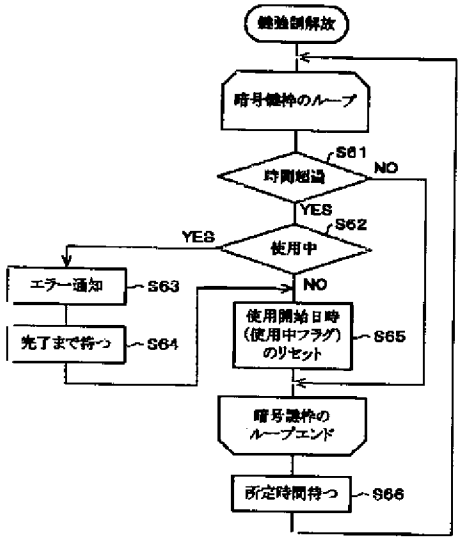
【図１２】

鍵No	暗号鍵	使用開始日時
0	・・・・・・・・・・・・・・・	200012150820
1	・・・・・・・・・・・・・・・	0
2	・・・・・・・・・・・・・・・	200012141557
	・・・・・・・・・・・・・・・	・・・・・
	・・・・・・・・・・・・・・・	・・・・・
N	・・・・・・・・・・・・・・・	0

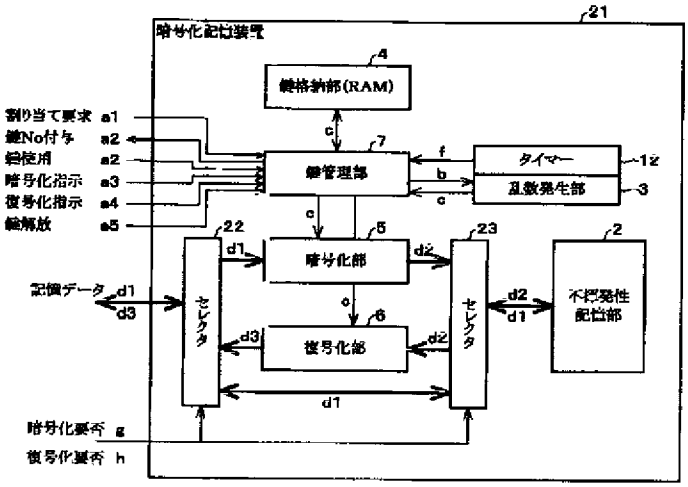
【図11】


鍵更新
次の鍵No計算
S51
使用中
S52
YES
NO
エラー通知
S53
完了まで待つ
S54
乱数生成
S55
値比較
S56
同
異
鍵設定
S57
現在鍵No更新
S58
一定時間待つ
S59

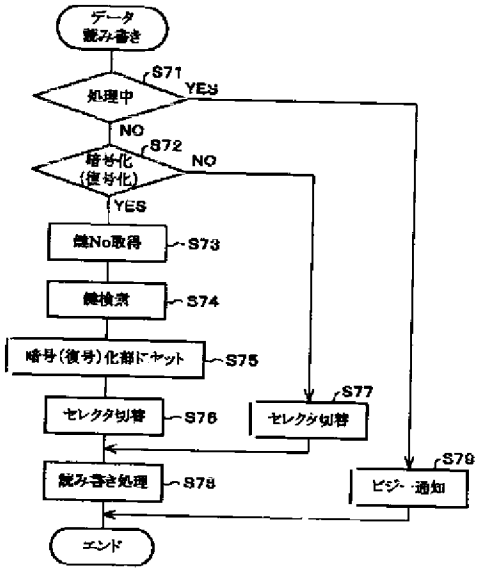
【図13】


鍵独占解放
暗号鍵枠のループ
時間超過
S61
NO
YES
使用中
S62
YES
NO
エラー通知
S63
完了まで待つ
S64
使用開始日時
(使用中フラグ)
のリセット
S65
暗号鍵枠の
ループエンド
所定時間待つ
S66

【図14】


21
暗号化記憶装置
4
鍵格納部(RAM)
割り当て要求 a1
鍵No付与 a2
鍵使用 a2
暗号化指示 a3
復号化指示 a4
鍵解放 a5
7
鍵管理部
タイマー
12
乱数発生部
3
22
23
2
5
暗号化部
6
復号化部
セレクタ
セレクタ
不揮発性
記憶部
記憶データ d1
d3
d2
d1
暗号化要否 g
復号化要否 h

【図15】



フロントページの続き

Fターム(参考) 5B017 AA07 BA07 CA16
5D044 AB01 BC01 BC04 CC04 DE49
EF05 GK12 GK17 HH15
5D110 AA13 DB05 DB11 DC03 DC19
DC22 DC27 DD13